THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

INTERIM TRANSPORTATION INFORMATION RISK ASSESSMENT REPORT

December 1997

1.0 INTRODUCTION

The President's National Security Telecommunications Advisory Committee (NSTAC), through the efforts of the Information Infrastructure Group (IIG), has been examining risks to the Nation's critical infrastructures for more than two years. In December 1996, the IIG created the Transportation Information Risk Assessment Subgroup to focus on the critical U.S. transportation infrastructure. This is an interim report of the subgroup. The contents of this report are based on subgroup meetings, research, and observations derived from the Transportation Information Risk Assessment Workshop conducted at U.S. Army Reserve Command, Ft. McPherson in Atlanta, Georgia on September 10, 1997. The members of the subgroup are listed in Appendix A.

1.1 Background

In January 1995, the Director of the National Security Agency briefed the NSTAC on threats to U.S. information systems and the need to improve the security of critical national infrastructures. The NSTAC principals discussed these issues and subsequently drafted a letter to the President in March of that year stating, "[t]he integrity of the Nation's information systems, both government and public, are increasingly at risk from intrusion and attack [and that] other national infrastructures [such as finance, air traffic control, power, etc.,] also depend on reliable and secure information systems, and could be at risk."[1]

The President replied to the NSTAC letter in July 1995, stating that he would "welcome NSTAC's continuing effort to work with the Administration to counter threats to our Nation's information and telecommunications system."[2] The President further asked, "the NSTAC principals-with input from the full range of users of the NII-to provide me with your assessment of national security and emergency preparedness requirements for our rapidly evolving information environment."[3] In 1995, the NSTAC formed the Information Assurance Task Force (IATF) to address these issues.

The IATF determined that three infrastructures-electric power, financial services, and transportation-were critically dependent on telecommunications and information systems. The IATF, renamed IIG in 1997 (see figure 1-1), has been conducting risk assessments of these three critical infrastructures. The IIG's electric power risk assessment was approved and forwarded to the President in March 1997. The financial services risk assessment was approved by the NSTAC principals in October 1997. (Copies of those reports can be obtained from the Office of the Manager, National Communications System, Customer Service and Information Assurance Branch, 701 S. Court House Road, Arlington, VA, 22204-2198.)

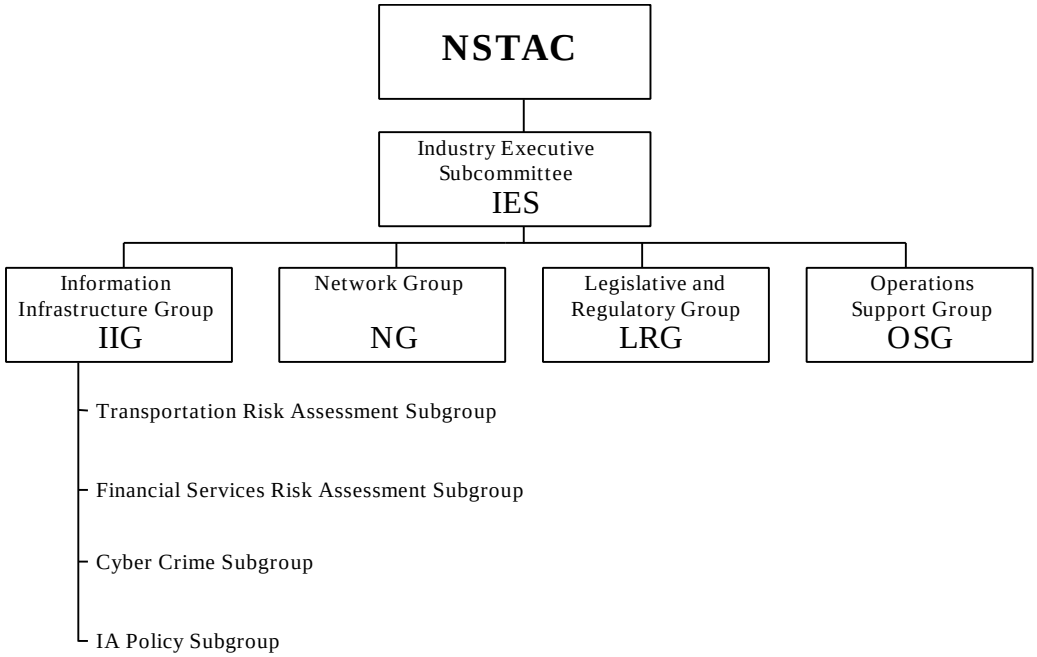
---

1 Letter from Mr. William Esrey, Sprint Corporation and Chair of the NSTAC, to the President of the United States, dated March 20, 1995.

2 Letter from the President of the United States to the NSTAC, dated July 7, 1995.

3 Ibid.

Figure 1-1. NSTAC Organizational Chart



The subgroup began work in December 1996 and since then has met with transportation industry representatives and concerned government officials in a variety of forums. In addition, the subgroup has coordinated its activities with the President's Commission on Critical Infrastructure Protection (PCCIP). The scope and complexity of the transportation industry necessitate a phased approach to accurately assess the risk to the infrastructure. The workshop represents the first significant step toward sharing information between the transportation industry and the telecommunications industry.

1.2 Risk Assessment Objectives

The subgroup's mission is to independently assess the risk of national level attacks on the transportation information infrastructure and networks that cause significant regional or national degradation or stoppage of the efficient movement of passengers or cargo. Based on NSTAC's continuing investigations into the vulnerabilities of public networks and information systems, the assessment will consider the risks to the transportation information infrastructure that derive from its dependence on information technology and the telecommunications infrastructure. As dependence on information systems within the transportation industry grows, so does the importance of reliable telecommunications systems. An increasingly complex and dynamic threat environment also raises additional concerns about an infrastructure that has already experienced a number of natural and manmade disruptions.

Accordingly, the subgroup identified the following objectives for its transportation information risk assessment effort:

- Assess the security and robustness of the transportation information infrastructure at the national level relative to the identified (i.e. known or experienced) threats to its networks and information systems
- Determine the risks to the transportation industry that derive from its dependence on information technology and the telecommunications infrastructure
- Examine the implications of trends regarding the industry's use of information systems and networks.
- Educate the transportation industry about information security threats and critical infrastructure interdependencies.
- Develop a working relationship between the transportation industry and the industries that compose other critical infrastructures with an impact on national security and emergency preparedness.

The following sections identify industry trends drawn from transportation industry background research and observations made by the subgroup at the Transportation Information Risk Assessment Workshop. Also outlined in the report are the next steps recommended by the subgroup to complete the final risk assessment.

2.0 INDUSTRY TRENDS

In addition to participating in the workshop, the subgroup met with a variety of public and private organizations and conducted research to determine significant trends in the transportation industry. The transportation industry is undergoing significant change, fueled by the increased use of information technology, expanding markets, and economies of scale.

2.1 Information Technology Growth

The transportation industry is becoming increasingly dependent on telecommunications and information technology. In 1995, transportation companies spent an estimated $16.3 billion on information technology to implement new business practices that bring information closer to the customer, reduce transit time, and cut transaction costs.[4] These services, largely the result of customer demand for information, increase transportation industry reliance on public networks, the Internet, electronic commerce, and electronic data interchange (EDI).

Because transportation firms operate in such a rapidly changing and expanding environment, they are interconnecting networks and expanding their use of open and proprietary

[4] Stephanie Stahl, "Information Is Part of the Package," *InformationWeek*, September 9, 1996.

information systems to remain competitive. For the majority of transportation firms, investment in EDI, database management, information tracking systems, and the Internet are a means to maintain a competitive advantage. United Parcel Service (UPS), for example, is one of nine U.S. corporations with an information technology budget greater than $1 billion per year.[5] The demand for information by transportation industry services consumers will continue to drive reliance on these systems.

In addition, the increase in the use of "just-in-time" (JIT) inventory creates the need for real time communication between freight transportation firms and customers. Inventory management, order requests, and payment transactions are increasingly transferred electronically by users of freight transportation services. To adequately support the timely physical movement of goods, the transportation industry must accommodate the business community as these types of transactions become commonplace. For the largest competitors involved, systems that provide immediate communication and service requirement data to customers have become an industry standard. Furthermore, competitive pressures now require companies to use intermodal forms of transportation to ensure the most timely, efficient, and cost-effective means of moving cargo from one point to another while making the entire process appear seamless to the customer.

Consumers are often the beneficiaries of the transportation industry's information technology investment. Users of passenger transportation can increasingly locate travel information, reserve tickets, and pay for service electronically. The airline industry is the leader in use of technology such as the Internet for customer services, but information for transit services, Amtrak schedules, and car rental reservations is also available. In addition, those companies involved in shipping cargo and packages are providing their customers with increased access to information regarding where a package is in transit and its expected time of arrival. Because these services are cost effective and increasingly serve as market differentiators for companies, they are expected to become more common and more highly developed.

Supervisory control and data acquisition (SCADA) systems, global positioning system (GPS) applications, and intelligent transportation systems (ITS) are perhaps the best examples of the industry's evolution toward increased reliance on information technologies.

2.1.1 Supervisory Control and Data Acquisition Systems

As with other infrastructures analyzed by the IIG, notably electric power, the transportation industry uses SCADA systems to automate operations that previously required manual control and monitoring. Most commonly used in the rail and pipeline industries, SCADA systems consist of sensors, computers, telecommunications links, and other servo-mechanisms that allow control centers to manage operating parameters throughout the system. These systems provide valuable data that are essential to regulate systems and ensure balance. In the pipeline industry, for example, SCADA systems permit remote control of valves, compressors, and other critical pipeline components. Often, these systems use microwave links due to the predominance of uninhabited and extremely rough terrain. Destruction of SCADA systems would result in

[5] Bob Violino, "The Billion Dollar Club," *InformationWeek*, November 25, 1996.

serious damage to pipeline operations.[6] In the rail industry, manual inspections are conducted to back up the automated system.

2.1.2 Global Positioning System

First developed by the U.S. Department of Defense (DoD), the satellite-based GPS is used for a variety of commercial transportation applications. Using triangulation principles and land-based receivers, GPS provides high levels of accuracy in determining Earth positions. A variety of systems that use GPS have been developed to improve the transportation of passengers and goods. According to the *THE* [Technical Horizons in Education] *Journal*, "the range of potential applications for GPS is limited only by a user's imagination."[7] In North America alone, the market for GPS applications is expected to grow from $366.2 million in 1996 to $3.5 billion by 2003.[8]

The use of GPS as a tracking tool is one important commercial application being developed. In the transportation industry, GPS allows freight carriers to improve delivery speed and accurately monitor shipments in crowded storage facilities and vehicles. This service is especially valuable for companies that transport large volumes of cargo in short periods of time.

A more important factor is that, from a safety and logistics standpoint, GPS technologies can facilitate the development of long-awaited intelligent railroads, highways, and airways. In the transit mode, some of these applications are being tested as a part of the ITS program to develop in-car traffic management systems and light-rail coordination applications. In aviation, GPS systems are being developed by government and industry to improve in-flight navigation systems, all-weather landing systems, and airport traffic surveillance. The pilot system developed to accomplish these goals, known as the Wide Area Augmentation System, or WAAS, is being tested by the Federal Aviation Administration (FAA). In addition, port authorities are examining the use of GPS to manage port traffic.

2.1.3 Intelligent Transportation Systems

Reliance on the highway system as the primary method of transportation has spurred the continued development of pilot programs for ITS throughout the country. These systems apply modern computer and communication technologies to transportation systems to improve traffic flow and vehicle capabilities. Products and services expected to be developed as a result of the ITS program include improved intermodal systems, intelligent traffic control, in-vehicle technologies, safety-enhancement products, and traveler advisory systems.

---

6 Reliability and Vulnerability Working Group, *NII Risk Assessment: A Nation's Information at Risk*, February 29, 1996.

7 Thomas A. Wikle et al., "Global Positioning System Instruction in Higher Education," *THE Journal (Technical Horizons in Education)*, December 1996.

8 "Global Positioning System Use On The Rise-Report," *Newsbytes News Network*, March 1997.

While the program is in the early stages of development and is subject to Federal Government funding constraints, private investment might help to expedite development of ITS applications. A market study commissioned by ITS America and the U.S. Department of Transportation found that if there is a national ITS deployment effort, the overall market for ITS products and services will total more than $430 billion over the next 20 years, most of which would come from spending in the private sector.[9] At present, ITS development is primarily divided into the following categories:

- Advanced Management Systems (ATMS)
- Advanced Traveler Information Systems
- Advanced Vehicle Control Systems
- Advanced Public Transportation Systems
- Commercial Vehicle Operation.

2.2 Intermodal Transportation

In broad terms, intermodalism refers to transportation that employs more than one mode to get passengers or goods from origination point to destination. This type of activity has increased in recent years because of the growth of cargo shipping and passenger travel miles. The use of standardized cargo containers and the construction of easily accessed ports and hubs are making intermodal methods more convenient and inexpensive, lowering intermodal handling costs. Companies that specialize in intermodal shipping and operate multiple fleets of vehicles in more than one mode are also becoming more common. Among the types of intermodal transport are truck and rail, truck and water, water and rail, and truck and pipeline.

In a more narrow sense, intermodalism refers to planned transportation methods and systems that provide easy physical transfer from one mode of transportation to another. This can be accomplished, for example, through the standardization of containers to decrease transfer time. Intermodalism also involves strategic placement of connection points to streamline connectivity between modes, such as adequate highway access to ports or bus feeder services. As integrators and other multimodal shipping firms respond to the demands for JIT delivery and mass customization on a national and international basis, intermodal activities will grow accordingly.

2.3 The Global Transportation Infrastructure

Increases in the frequency of international travel and the level of cargo transport will extend the national transportation infrastructure worldwide. One of the most likely sources for such increases, the passenger airline industry, expects growth of 3 to 4 percent in international travel both in and out of the United States.[10] Recent liberalization of U.S./Canada and U.S./Mexico restrictions could enhance transportation between these countries for all modes.

---

9 "Strong Federal Role Sought For Intelligent Transportation," *ITS America Online*, March 6, 1997.

10 Standard & Poor, *Airlines Industry Survey*, March 27, 1997.

A critical factor is that the U.S. transportation industry is growing more dependent on international sources to support consumption of oil and energy. This trend has grown over the last decade and is likely to continue, with transportation accounting for about two-thirds of the country's total oil consumption.[11] Although the industry has attempted to address such a reliance on energy use through efficiency regulations and technological improvements, consumption levels of foreign energy sources by the transportation industry remain a concern.

3.0 WORKSHOP PROCEEDINGS

The Transportation Information Risk Assessment Subgroup determined that a workshop that included representatives from all transportation modes would best meet the goal of assessing the risk to all components of the transportation information infrastructure. To that end, a range of transportation industry and regulatory representatives were targeted for attendance at the 1-day workshop at Fort McPherson. Prior to the workshop, prospective participants were sent an invitation packet that defined the following workshop objectives:

- Determine the interdependencies of the transportation information industry infrastructure
- Determine how different modes of the transportation industry share information
- Determine the coordination mechanisms between transportation modes, other infrastructures, and the Government
- Determine the risks to the information infrastructure and the level of understanding the Government has regarding transportation industry vulnerabilities.

A fictional threat scenario, designed to reflect the composition of the transportation industry in the Southeast region of the United States, was also included in each information packet to facilitate workshop discussion. The threat scenario is attached as Appendix B to this document.

Industry and government regulatory agency representatives from the rail, transit, pipeline, and airline modes attended the workshop. Southeastern United States port authorities and multimodal integrator corporations were also represented. Participants attended a morning plenary session that included the following briefings:

- **Dr. Dan Wiener II,** Unisys Federal Systems
  Overview of the President's NSTAC. Dr. Wiener provided a brief history of the NSTAC, as well as an explanation of current membership and structure. He explained the interest of the NSTAC in critical infrastructure security and, in particular, the transportation industry.

[11] U.S. Department of Transportation, Bureau of Transportation Statistics, *Transportation in the United States, A Review,* Washington, D.C., 1997.

- **Mr. Guy Copeland,** Computer Sciences Corporation
  NSTAC Risk Assessments. Mr. Copeland focused on the NSTAC's past involvement in critical infrastructure risk assessments and the results and observations from completed reports. Mr. Copeland also addressed past and current information security studies conducted by the NSTAC on cyber crime and security. He also explained the Information Systems Security Board (ISSB) concept.

- **Rear Admiral Paul Pluta,** U.S. Coast Guard
  Department of Transportation (DOT) Support. Rear Admiral Pluta highlighted the role of the DOT Office of Intelligence and Security (OIS) in providing support for transportation-related intelligence and security programs and issues. He summarized the DOT *Surface Transportation System Vulnerability Assessment* study and provided statistical information on the status of terrorist threats to transportation.

.

- **Mr. Jay Manning,** Federal Bureau of Investigation (FBI)
  International Terrorism. Mr. Manning discussed the profile of contemporary terrorist threats and the efforts of the FBI Counterterrorism Program to prevent and, when necessary, investigate terrorist incidents. He also provided information on the role of technology and information warfare in future transnational terrorist activities.

- **Mr. Ken Piernick,** FBI
  Domestic Terrorism. Mr. Piernick briefed workshop participants about the status of domestic terrorism and provided a description of the likely demographics of persons involved in domestic terrorism activity. Using real examples, Mr. Piernick summarized the likelihood of threats to the transportation industry and the motivations behind such threats.

- **Mr. James Werth,** FBI
  The Infrastructure Protection Task Force (IPTF) and Computer Incident and Infrastructure Threat Assessment Center (CITAC). Mr. Werth described the backgrounds and missions of the IPTF and CITAC. Specifically, he explained the effort to coordinate existing expertise within and outside the Government to protect critical national infrastructures from cyber threats.

Following the briefings, the participants were divided into two teams to discuss the effect of the threat scenario prepared by the subgroup. Members of the subgroup facilitated the discussions of topics that included-

- **Disaster recovery.** The plans in place to continue operation of the transportation information infrastructure during a loss of telecommunications and related infrastructure service.

- **Network security.** The methods by which individual information systems and networks, both public and private, are protected from intrusion.

- **Reporting requirements.** The amount and type of information reported to regulatory authorities, and the ways in which this information can be made useful for both industry and government.

- **Threat awareness.** Industry awareness of the types, sources, and detection of cyber threats to information systems and the physical and cyber infrastructure.

- **Corporate information security authority.** The role and level of authority of industry information security officials within individual transportation corporations.

- **Use of telecommunications.** General industry reliance on the telecommunications industry to provide basic service to customers.

- **Regulatory oversight.** The coordination and relationship between the regulatory authority and the industry as a whole, each specific mode, and individual corporations.

.

- **Trends.** The direction of the industry as both a critical infrastructure and an essential component of business operations.

- **Intermodal transportation.** The amount of intermodal service at present and the unique physical and information security issues presented by the increased use of such service.

- **Insider threat.** The security implications which are presented by a hostile or compromised insider with knowledge of a firm's vulnerabilities and the precautions taken to prevent such a threat.

- **Information sharing.** The importance and practice of information sharing within an industry or mode through the use of an industry association, or information sharing between counterparts from different firms with similar security responsibilities.

- **Intrusion detection.** The methods for detection of intrusion into information systems and the number of intrusions encountered.

- **Relevant labor issues.** The potential for labor obstacles, such as an increase in hours worked, that may result if an emergency occurs, and the plans to account for these obstacles.

- **Infrastructure interdependencies.** The reliance of the transportation infrastructure on other critical infrastructures other than telecommunications (e.g., electric power, financial services).

4.0 FINDINGS AND OBSERVATIONS

The workshop provided an excellent forum to discuss the topics listed above, but time constraints and the amount of participation limited the scope of data collection efforts. The following section describes the initial findings and observations of the subgroup. These findings are based solely on the workshop discussion and, therefore, may reflect a regional perspective rather than be representative of the entire infrastructure. Furthermore, it should be noted that all workshop discussions were recorded on a nonattribution basis.

4.1 Information System Security

Members of the subgroup made the following observations about the security of and reliance on information networks in the transportation industry:

- **Uneven knowledge of telecommunications and information systems.** Although many of the industry representatives acknowledged that their firms were moving towards open systems, most were unaware that voice, data, and control information often travels over the same telecommunications paths. This interdependence can affect quick backup procedures during network outages. Furthermore, most representatives did not view technologies that use SCADA systems and GPS applications as potential vulnerabilities.

- **Comfortable with present information security systems.** Industry representatives felt that a good portion of data is still transferred over closed networks and is, therefore, relatively safe from intrusion. Of those firms that use open networks, most felt their systems provided adequate protection from intrusion, despite estimates from one industry representative that up to 200 attempts at infiltration are detected per week.

- **Moving toward automated systems.** The transportation industry, notably rail and pipeline, is growing more reliant on automated systems such as SCADA. Industry representatives reported a variety of security measures associated with these systems, but acknowledged the increased use of digital signal transmission.

- **Uncertain about system vulnerabilities.** Despite their comfort with individual security systems, workshop participants communicated an uncertainty about the reliability of network security ratings. Of the firms that reported undergoing vulnerability assessments and/or penetration testing, most felt that the information was out of date or incomplete and that they were always testing for past faults. The subgroup also observed that the industry relied on auditing firms for security recommendations, and that guidelines or oversight about best practices for ensuring secure systems would be helpful.

4.2 Emergency Preparedness and Contingency Plans

The following observations were made by the subgroup concerning the emergency preparedness contingency plans of the transportation industry:

- **Transportation is dependent on other infrastructures.** Industry representatives agreed that other infrastructures, most notably power and telecommunications, were instrumental in the transportation industry's ability to carry out emergency plans. Although operations could continue in some manner without these infrastructures, a prolonged loss of either of these services would deplete backup reserves of energy and personnel, and certainly cause long-term difficulties.

- **Industry familiarity allows communication and planning.** During regional disturbances of telecommunications service, most representatives felt that coordination could be easily achieved between firms within the same transportation mode. Because the appropriate counterparts at each firm communicate with one another regularly, organization and sharing of resources would not be problematic. In the rail industry, for instance, this cooperation occurs at the highest corporate levels, often between chief executive officers (CEO).

- **Plans exist but are not exercised.** The transportation industry plans for a loss of telecommunications service or other infrastructure, but these plans are not exercised regularly. Furthermore, arrangements for sharing resources during a service loss are not explicit or prenegotiated to streamline coordination.

4.3 Threat and Security Information Sharing

Industry representatives communicated the following points concerning sharing threat information within the industry, with other industries, and with government officials:

- **Government data-sharing viewed negatively.** Most industry representatives viewed providing security information to the Government as expensive and time consuming. The present level of reporting to regulatory agencies was deemed to be appropriate and not overly burdensome, but firms communicated that they gained little benefit from such activity. In particular, they emphasized it was equally important for industry to be forwarded information on threats to their physical and information infrastructures.
- **Industry associations are important.** The role and importance of industry associations in coordinating activities and obtaining information were clear. Some of these associations operate central electronic databases for use by firms. The subgroup observed the need to include such associations in further discussions of information sharing and reporting, which should be done at the CEO level.

- **Interest was expressed in gaining threat information.** No industry representatives present at the workshop reported ever having received threat information from Federal

Government sources, although most thought this information would be useful. Rather, such information was thought to be more likely received through industry associations or local law enforcement sources, if at all.

- **The workshop resulted in greater awareness.** Industry officials agreed that greater awareness of information security threats was needed and advised that discussion continue with the telecommunications industry and, potentially, government. Members of the subgroup observed a significant increase in understanding and interest in infrastructure protection by the workshop participants. Furthermore, the presentation of a National Coordinating Mechanism (NCM) concept briefing by the NSTAC members provided a first step toward discussing cross-infrastructure issues and concerns.

5.0 NEXT STEPS

The subgroup believes that further action and outreach with the transportation industry are needed before a comprehensive risk assessment and recommendation can be developed. Although the workshop was brief, a great deal of information was exchanged on the transportation industry's exposure to risks through its use of telecommunications and information systems. Although this exchange was valuable, clearly there is a need to gather more detailed information to develop a complete and accurate picture of the risks to the transportation industry and to achieve the following goals:

- **Collect data and information from underrepresented modes.** Several transportation modes, specifically, airlines, multimodal sources, and mass transit entities, were missing or underrepresented at the workshop. In addition, the workshop focused on the southeastern United States, which precludes any national-level conclusions.

- **Discuss intermodal issues.** Industry representatives did not adequately discuss intermodal issues. The subgroup observed that intermodal transportation is often complicated and difficult to assess from a security standpoint. Intermodal exchanges represent the points of commonality between transportation modes and possibly provide the best understanding of the vulnerabilities for the infrastructure as a whole. Future information-gathering efforts should use creative methods to stimulate intermodal discussion and analysis.
- **Facilitate greater information exchange.** Members of the subgroup and workshop participants agreed that representatives from the transportation industry would benefit from further information exchange. Future events will allow the NSTAC and other appropriate government agencies to inform and discuss information-based threats and vulnerabilities with transportation officials.

- **Interface with industry associations.** Several workshop participants identified the importance of the industry associations in sharing information. In light of this

observation, the subgroup must build relationships with these associations to gain a full understanding of the transportation information infrastructure.

- **Focus on modes and organizations with national impact.** To meet the risk assessment goal of assessing the robustness of the national transportation information infrastructure, future efforts of the subgroup should focus on gaining information from organizations or modes with a national impact. Although input from localized or regional transportation organizations is valuable, a concentration on national security and emergency preparedness and security must be maintained.

6.0 RECOMMENDATIONS

Based on the aforementioned next steps, the subgroup recommends the following:

- A second transportation infrastructure workshop should be held to facilitate information exchange, further investigate intermodal transportation and transportation infrastructure dependency issues, and finish the data collection effort to complete the subgroup's task.

- The workshop should involve national transportation industry representatives, including relevant industry associations.

APPENDIX A

Transportation Risk Assessment Subgroup Members

Transportation Risk Assessment Subgroup

Unisys	Dr. Dan Wiener, Chair
CSC	Ms. Deborah Jacobs
CSC	Mr. Guy Copeland
CSC	Mr. Richard Swanson
DOT	Mr. Tim Custer
GTE	Mr. Lowell Thomas
GTE	Ms. Ernie Gormson
Lockheed-Martin	Mr. Bruce Wallachy
NTA	Mr. Bob Burns
Raytheon/E-Systems	Mr. Bob Tolhurst
TRW	Mr. Bob Lentz
Unisys	Ms. Mary Dale

APPENDIX B

Transportation Information Risk Assessment Workshop Scenario

Imagine we are sitting in this room less than two years from now and the President has asked us to provide transportation system recommendations to the National Security Council on how to best deal with the following scenario. As major transportation providers and users, your inputs are very important to the National Security Council and the President. We appreciate your attendance and input.

Today is December 20, 1999; both the northeastern United States and Europe have had record cold for this early in the winter. Japan and Germany, with 90% and 50% of their oil coming from the Persian Gulf region respectively, are down to 25-30 days of fuel oil reserves. Any slowdown of oil flow from the Persian Gulf for even a few days will therefore have immediate and disastrous consequences for two of the three main driving wheels of the global economy. Damage to the US economy will be slower in coming but no less profound. The following events brought us to this crisis and will provide a framework for today's discussions.

Despite Iran's 1997 election of an apparent moderate to lead it into the 21st century, it has not softened its basic anti-West, anti-US stand. Acts of Iranian-sponsored terrorism have continued throughout the Middle East, aimed at splitting the United States and its allies in the region. US trade sanctions against Iran remain in place, but we have had only limited success in persuading others to follow suit. The Iranian economy has been slowly recovering from the excesses of previous regimes, but it is cash starved. Iran had planned to solve this problem by charging transit fees on the vast amounts of oil soon to be reaching the world market via pipelines from new fields in and around the Caspian Sea, but for various reasons those pipelines are being routed elsewhere.

Six months ago, during annual troop maneuvers, Iran moved about 50,000 troops to the Bandar Abbas area; indications are that they are there to stay. As you know, a number of small islands dot the Strait of Hormuz. These islands have been claimed by Iran despite the objections of her neighbors. Iranian occupation and fortification of these islands has had the effect of raising the level of threat in one of the world's most strategic straits. Iran has also more than doubled the number of fast patrol boats in the area in recent weeks; many of these craft are capable of laying mines.

Simultaneously, on the diplomatic front, Iran has been conducting a campaign to justify its right to control the passage of ships through the Strait of Hormuz on the grounds that the main shipping channel passes through Iranian "territorial waters." The conclusion is inescapable that Iran is setting the stage to attempt to exercise control in the strait and is prepared to use military force if challenged. Iran's most probable tactic will be to mine all but a narrow channel through the strait and to use its patrol boats to stop and board ships in transit, charging a fee for safe passage. The duration of any closure, and the amount of tariff that Iran might impose, are unknown at this time. The United States, and most other members of the United Nations, have made it clear that this would be a violation of international law and would result in "immediate and appropriate" action. The Commander in Chief of the United States Central Command (CINCCENT) has been directed to prepare a modification of an existing contingency plan. CINCCENT requested, and was given authority, to move a carrier battle group into the northern

Indian Ocean, deploy two squadrons of F-16's to the region, move several Army and Marine units to theater, and to raise the alert posture of many other units in all the services.

The President has authorized the use of national oil reserves as the world oil supply has tightened and prices have begun to climb. Spot prices for Saudi oil have gone as high as $35 per barrel and other markets have followed suit as Japan and Germany have sought other oil sources.

Following the US announcement on 15 December that troops would begin moving towards the theater, a series of events occurred that many people believe to be the work of Iranian agents, although Iran had not claimed responsibility at that time. A shutdown of the main planning and tracking computer of a major southeast rail provider occurred; a computer worm is thought to be the cause. A logic bomb caused an unplanned shutdown of three power plants in Georgia; the resulting overload caused a cascading power failure through most of Georgia, South Carolina, and parts of Alabama. A computer virus in both the Atlanta and Jacksonville air traffic control centers caused a scrambling of the air traffic picture throughout the entire southeast. Air traffic controllers reduced the number of flights in the region to one-half of normal as a safety precaution until they can be certain that they have found all the problems. Calls to airlines and relatives have put an extremely high stress on telecommunications systems as people scramble to adjust their holiday plans. An as yet unexplained loss of control of a commuter rail switching center in Jacksonville, Florida, caused the shutdown of a commuter rail system in northern Virginia. In all these instances there is evidence of electronic intrusions into computer centers; the source of the intrusions is uncertain, but all indicators point towards Iran as the sponsor.

The power outages in the South caused heaters at a number of natural gas pumping stations to be off long enough to freeze some valves and pumps, which may not work once power is restored. Many natural gas providers are indicating that they may have to shut down because they are unable to track where their gas is going. The situation is already worse than in the winter of 1989.

On 17 December, the President issued a strongly worded denunciation of Iran's actions at the UN. He requested that state and local governments increase their police patrols to be on the lookout for suspicious activities around major infrastructure locations. He also put national guard and regular military units on heightened alert. No additional troop movements have been ordered. Later on the 17th, an Iranian patrol boat stopped a Very Large Crude Carrier (VLCC) carrying 2.5 million barrels of crude oil in the Strait of Hormuz and refused to let it proceed until its owners pay a $5.00 per barrel tariff for safe passage. Iran announced that it has mined the strait and any ship not paying its tariff will not be allowed to pass.

Japan and Germany formally complained to the UN on December 18th, and requested US assistance in reopening the strait before their oil situation becomes more critical than it already is. CINCCENT was ordered to begin moving the units called for in his contingency plans and to standby for execution of his op-plan if the situation can not be resolved within the next two days.

Yesterday evening a massive power outage occurred in Washington, D. C., northern Virginia, and Maryland. Acts of sabotage at three critical substations were quickly identified as

the cause. A passenger traveling through Harts field Airport collapsed while waiting for a connecting flight. Public health officials arrived to find several other travelers already experiencing symptoms of whatever highly contagious disease the first sick passenger had. Public health officials recommended closing the airport and quarantining the passengers there. All passengers who arrived in Atlanta on the flight with the sick man are being sought to place them in quarantine, but many have already left on connecting flights. A mass transit commuter train derailed in Atlanta during the evening rush hours as a result of a switch being set wrong; an intrusion into the rail system's computers was detected, but no one knows yet if that was the cause of the mis-set switch.

Yesterday morning, ten minutes before a train filled with troops and equipment would have arrived at a key rail bridge leading to the Savannah port, the bridge was blown up. The train was stopped in time, but it had passed the last point at which it could have been switched onto another line. The rail lines, trucking companies, United States Transportation Command (TRANSOM), and state officials began looking at rail, truck, and road capacities to determine the best way to reroute. At 1000 hours, a freighter leaving Savannah exploded in a huge fireball and sank in the entrance to Savannah harbor. Iranian terrorists claimed responsibility and stated that any vessels attempting to leave Savannah carrying military cargo will meet with a similar fate. It is not yet known if a mine was the cause of the explosion. In Atlanta, a building containing a key telecommunications switch in it was evacuated for a bomb threat. When the building reopened, technicians discovered that the computer controls for the switch had been tampered with; telephone service to the region is still being disrupted.

By noon, financial centers in Tokyo, Europe, and New York had all reported intrusion attempts which they believe have not been successful yet, but which are continuing through several sources, none of which have been located at this time.

At the UN, the Iranian ambassador delivered a speech full of rhetoric demanding that the United States stay out of its affairs and indicating that the Iranian government will take all actions available to them to deter the United States from deploying troops or from stopping its "legal" tariff collection within its territorial waters.

The massive US troop movement is being slowed by the loss of the key rail bridge and the blocking of Savannah harbor, but workarounds have now been planned. New bomb threats and the destruction of several highway bridges further complicates the problem. The President may declare a state of emergency before the day is over. CINCCENT is asking for priority over all commercial shipping from key ports and airfields. Additionally, he is requesting that more trucking be made available to move troops and equipment to their embarkation sites. TRANSOM is trying to coordinate with the states for increased weight limits on their highways and for information on overpass clearances which may not meet the requirements of the National Highway Act. This information is proving very difficult to obtain quickly.

Meanwhile, world oil prices are rising hourly and stock markets are reporting record declines in extremely heavy trading. Calls to shut down the New York Stock Exchange are coming in hot and heavy with the suggestion that it would be justified by ongoing attempts to

intrude into the exchange's computers. Television and radio broadcasts are being disrupted by the power outages in the South and in the Washington area. The public outcry is escalating rapidly in the United States as well as in Europe and Japan. Air, rail, and road traffic are being severely affected, and some trucking companies are saying that they will not endanger their drivers until they can be assured that bridges have been checked for explosives and that National Guard or other units are providing 24 hour protection of the bridges. The major telecommunications providers are reporting that only 25 percent of the calls being placed into, or out of, the Atlanta and Savannah areas are getting through. The President and the Governor of Georgia have gone on television and radio to request that people make only essential calls until the various national and regional disruptions and deployments have been straightened out. The President is also seeking to reassure the public that our infrastructures will be protected and that electricity, heat, and groceries on supermarket shelves are high on his priority list. Predictably both government and industry are being severely impacted by these events.

This scenario was designed to represent credible events which could seriously stress transportation and information networks. All of these events may not seem to be totally realistic, but we do not want to focus on that, rather we want to use the questions below to provide a framework for open and useful discussion.

WORKSHOP FRAMING QUESTIONS

1. If the situation postulated in the scenario is not one which would cause you serious stress, what scenario or events would most impact the continuity of your business operations? What actions might your organization and/or the government implement to mitigate those impacts?

2. How would events outlined in our scenario or yours impact the conduct of your business? How would key systems and components be stressed?

3. To what extent are the businesses or functions under your responsibility dependent upon the national information infrastructure and its components (e.g., computers, automated control systems, voice and data communications, Internet, and information security)?

4. The scenario deliberately postulates compounding actions, outages, and stresses across all modes of transportation. Do you interact with other industry or Government entities to discuss contingency plans for these types of situations? Are any such plans designed to address infrastructure-wide (i.e., intermodal) concerns?

5. Are coordinating mechanisms in place today sufficient to specifically address intermodal and information systems issues? How do Government and industry share information on threats and vulnerabilities?

6. In deploying troops or moving commercial cargo, ports and airports represent potential bottlenecks. How does the increasing use of intermodal transportation assets and information systems to route and track cargo impact ports and airports? Are they reliant on the information or other critical infrastructures (e.g., electric power)? Would denial of service attacks against electric power or telecommunications disrupt essential port and airport activities?